

Delphion

[RESEARCH](#)
[INTEGRATED IAM](#)
[SERVICES](#)
[INSIDE DELPHION](#)
[Log Out](#)
[Work Files](#)
[Saved Searches](#)
[My Account](#) | [Products](#) | [News](#) | [Events](#)
[Search: Quick/Number Boolean Advanced](#)

The Delphion Integrated View: INPADOC Record

Buy Now: [More choices...](#)

Tools: Add to Work File: [Create new Work File](#)

View: Jump to: [Top](#)

☒ Go to: [Derwent...](#)

☒ [Email](#)

🔍 Title: **FR2782224B1: PROCEDE ET DISPOSITIF D'INSERTION ET DE DECODAGE D'UNE MARQUE DANS DES DONNEES NUMERIQUES**

🔍 Country: **FR France**

🔍 Kind: **B1 Patent of Invention (Second Publication)** ¹ (See also: [FR2782224A1](#))

🔍 Inventor: **DONESCU IOANA;**

🔍 Assignee: **CANON KABUSHIKI KAISHA, Japan**
[News, Profiles, Stocks and More about this company](#)

🔍 Published / Filed: **Nov. 3, 2000 / Aug. 6, 1998**

🔍 Application Number: **FR1998000010149**

🔍 IPC Code: **H04N 1/32; H04N 7/08;**

🔍 ECLA Code: **G06T1/00W; H04N1/32C19;**

🔍 Priority Number: **Aug. 6, 1998 FR1998000010149**

🔍 Family:

PDF	Patent	Pub. Date	Filed	Title
	JP2000101828A2	April 7, 2000	Aug. 6, 1999	METHOD AND SYSTEM FOR INSERTING TO AND DECODING DIGITAL DATA WATERMARK FOR DIGITAL DATA
	JP0101828A2	April 7, 2000	Aug. 6, 1999	METHOD AND SYSTEM FOR INSERTING TO AND DECODING DIGITAL DATA WATERMARK FOR DIGITAL DATA
	FR2782224B1	Nov. 3, 2000	Aug. 6, 1998	PROCEDE ET DISPOSITIF D'INSERTION ET DE DECODAGE D'UNE MARQUE DANS DES DONNEES NUMERIQUES
	FR2782224A1	Feb. 11, 2000	Aug. 6, 1998	PROCEDE ET DISPOSITIF D'INSERTION ET DE DECODAGE D'UNE MARQUE DANS DES DONNEES NUMERIQUES
	FR2782223B1	Nov. 3, 2000	Aug. 6, 1998	PROCEDE ET DISPOSITIF D'INSERTION ET DE DECODAGE D'UNE MARQUE DANS DES DONNEES NUMERIQUES
	FR2782223A1	Feb. 11, 2000	Aug. 6, 1998	PROCEDE ET DISPOSITIF D'INSERTION ET DE DECODAGE D'UNE MARQUE DANS DES DONNEES NUMERIQUES
6 family members shown above				

THIS PAGE BLANK (USPTO)

①⑨ RÉPUBLIQUE FRANÇAISE
INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE
PARIS

①① N° de publication :
(à n'utiliser que pour les
commandes de reproduction)

2 782 224

②① N° d'enregistrement national : 98 10149

⑤① Int Cl⁷ : H 04 N 1/32, H 04 N 7/08

⑫

DEMANDE DE BREVET D'INVENTION

A1

②② Date de dépôt : 06.08.98.

③① Priorité :

④③ Date de mise à la disposition du public de la
demande : 11.02.00 Bulletin 00/06.

⑤⑥ Liste des documents cités dans le rapport de
recherche préliminaire : *Se reporter à la fin du
présent fascicule*

⑥① Références à d'autres documents nationaux
apparentés :

⑦① Demandeur(s) : CANON KABUSHIKI KAISHA — JP.

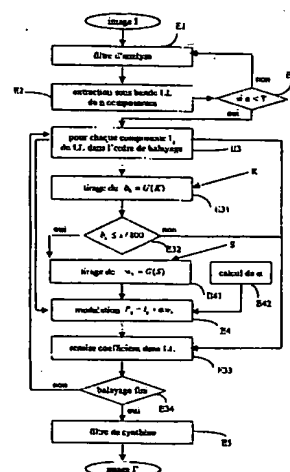
⑦② Inventeur(s) : DONESCU IOANA.

⑦③ Titulaire(s) :

⑦④ Mandataire(s) : RINUY SANTARELLI.

⑤④ PROCÉDE ET DISPOSITIF D'INSERTION ET DE DECODAGE D'UNE MARQUE DANS DES DONNÉES NUMÉRIQUES.

⑤⑦ Un procédé d'insertion d'une marque dans des données numériques (I) comporte les étapes de décomposition spectrale multi-résolution (E1) des données numériques (I); d'extraction (E2) des composantes de plus basse fréquence; de choix (E3) d'un sous-ensemble des composantes de plus basse fréquence; de modulation (E4) des composantes dudit sous-ensemble pour insérer l'information supplémentaire (S); et de recombinaison spectrale multi-résolution inverse (E5) des données numériques marquées (I').



FR 2 782 224 - A1



5

10 La présente invention concerne un procédé et un dispositif d'insertion d'une information supplémentaire, telle qu'une marque secrète, dans des données numériques.

Elle concerne également un procédé et un dispositif de décodage d'une telle information supplémentaire insérée par le procédé d'insertion
15 conforme à l'invention.

Elle s'inscrit de manière générale dans le domaine technique du marquage (en anglais watermarking) des données numériques.

La prolifération des échanges de données multimédia numérisées par voie informatique favorise la création et la distribution de copies illicites, et
20 d'une façon générale, la manipulation illégale de ces données.

Le marquage des données numériques consiste à insérer une marque directement dans les données numérisées. L'insertion de cette marque est assimilée au codage d'une information supplémentaire dans les données numériques.

25 Un marquage classique consiste à insérer un logo visible lorsque les données numériques sont des images. Néanmoins, cette marque est facile à enlever pour un utilisateur qui souhaite manipuler illégalement cette image.

On utilise alors fréquemment une marque dite invisible qui doit présenter les facteurs de qualité suivants :

30 Cette marque doit être imperceptible, c'est-à-dire que l'insertion d'une telle marque doit préserver la qualité perceptuelle des données numériques, par exemple, la qualité visuelle pour des images ou la qualité

auditive pour des données audio. L'imperceptibilité de la marque rend en outre son piratage plus difficile.

Cette marque doit également être indélébile, c'est-à-dire être statistiquement indétectable dans les données numériques marquées afin de
5 résister aux attaques intentionnelles pour détruire cette marque.

Cette marque doit en outre être robuste aux traitements classiques appliqués aux données numériques, tels que compression et décompression, transformation numérique / analogique, filtrage...

Cette marque doit enfin être fiable, c'est-à-dire permettre une
10 décision fiable quant à l'existence ou non d'une marque donnée dans des données numériques données.

Les procédés d'insertion existants sont mis en œuvre en modifiant les hautes ou moyennes fréquences contenues dans les données numériques, notamment lorsque ces données numériques représentent une image. Le fait
15 de modifier uniquement les hautes fréquences permet de garantir l'invisibilité de la marque insérée. Cependant, ces marques sont peu robustes aux distorsions, et en particulier ne résistent pas aux compressions classiques qui quantifient largement les composantes spectrales de moyenne ou haute fréquence.

On connaît un procédé d'insertion d'une marque, décrit dans la
20 Demande de Brevet européen N° 0 766 468 au nom de NEC CORPORATION, dans lequel on réalise une transformation fréquentielle des données numériques avant d'insérer l'information supplémentaire dans des composantes significatives perceptuellement. Une transformation fréquentielle inverse permet d'obtenir les données numériques marquées. Une transformée en cosinus
25 discrète ou une décomposition en sous-bandes par une transformation en ondelettes discrète peuvent être appliquées sur l'ensemble des données numériques, par exemple une image. On module ensuite par exemple les N plus grandes composantes fréquentielles de la transformée pour insérer l'information supplémentaire. La sélection des composantes significatives
30 perceptuellement est cependant difficile à mettre en œuvre.

La présente invention a pour but principalement d'améliorer les procédés d'insertion existants et d'accroître la qualité de la marque insérée, notamment en terme d'imperceptibilité et de robustesse.

Conformément à l'invention, le procédé d'insertion d'une information
5 supplémentaire, telle qu'une marque secrète, dans des données numériques, est caractérisé en ce qu'il comporte les étapes suivantes :

- décomposition spectrale multi-résolution des données numériques ;
- extraction des composantes de plus basse fréquence ;
- 10 - choix d'un sous-ensemble des composantes de plus basse fréquence ;
- modulation des composantes dudit sous-ensemble pour insérer l'information supplémentaire ; et
- recomposition spectrale multi-résolution inverse des données
15 numériques marquées.

Corrélativement, un dispositif d'insertion d'une information supplémentaire, telle qu'une marque secrète, dans des données numériques, est caractérisé en ce qu'il comporte :

- des moyens de décomposition spectrale multi-résolution des
20 données numériques ;
- des moyens d'extraction adaptés à extraire des composantes de plus basse fréquence ;
- des moyens de choix pour choisir un sous-ensemble des composantes de plus basse fréquence ;
- 25 - des moyens de modulation des composantes dudit sous-ensemble pour insérer l'information supplémentaire ; et
- des moyens de recomposition spectrale multi-résolution inverse des données numériques marquées.

Selon l'invention, un choix préalable est réalisé à travers la
30 décomposition spectrale multi-résolution et l'extraction des composantes de plus basse fréquence, ce qui permet de localiser les composantes modulables de façon automatique dans une zone du spectre, et non dans tout le domaine

spectral. Ceci est particulièrement bien adapté à la vérification de la marque insérée, par exemple lorsqu'il s'agit de vérifier des droits d'auteur sur une image numérisée.

En outre, le choix préalable d'une sous-bande spectrale de plus
5 basse fréquence, dans laquelle certaines composantes sont modulées pour introduire l'information supplémentaire, permet de sélectionner de manière systématique des composantes fréquentielles robustes à divers algorithmes de compression des données numériques et notamment aux traitements classiques de compression et décompression utilisés pour les images
10 numériques.

La Demanderesse a montré, alors qu'il est couramment admis que les composantes basses fréquences n'admettent que de très faibles modulations sans distorsions visuelles importantes sur l'image reconstruite, qu'il est possible d'ajouter une information supplémentaire en insérant un signal de
15 puissance significative sur ces composantes de manière imperceptible à condition d'atteindre un niveau de résolution suffisamment faible lors de la décomposition spectrale multi-résolution.

Selon une version préférée de l'invention, le niveau de décomposition spectrale multi-résolution est prédéterminé de telle sorte que le
20 nombre de composantes de plus basse fréquence est compris entre 8x8 et 32x32.

La Demanderesse a montré de manière empirique qu'une sous-bande de cette taille convenait particulièrement bien à l'insertion d'une information supplémentaire tout en garantissant l'imperceptibilité de cette
25 information supplémentaire.

En outre, les méthodes proprement dites d'insertion du signal représentatif de l'information supplémentaire et de détection de ce signal seront particulièrement efficaces grâce à la réduction importante de l'espace modulable par rapport à la dimension des données numériques initiales.

30 Selon une version avantageuse de l'invention, particulièrement bien adaptée à l'insertion d'une marque dans une image numérique, à l'étape de décomposition spectrale, la décomposition spectrale est réalisée par une

transformation en ondelettes discrète, et à l'étape d'extraction, on choisit les composantes de la sous-bande d'approximation.

Selon une autre version avantageuse de l'invention, et alternativement à la version précédente, à l'étape de décomposition spectrale, 5 les données numériques sont décomposées de manière itérative en une version d'approximation correspondant à un filtrage passe-bas et un sous-échantillonnage des données numériques ou d'une version d'approximation précédente et une version de détail correspondant à la soustraction de la version d'approximation des données numériques ou de la version 10 approximative précédente, et à l'étape d'extraction, on choisit les composantes de la version d'approximation.

Cette décomposition suivant un schéma pyramidal est également particulièrement bien adaptée à la décomposition d'une image en sous-bandes d'approximation successives et garantit une reconstruction parfaite de l'image 15 après insertion du signal représentatif de l'information supplémentaire.

Selon une version préférée de l'invention, à l'étape de modulation, les composantes dudit sous-ensemble sont modulées par addition d'une valeur de modulation générée par une fonction pseudo aléatoire initialisée par un signal numérique représentatif de l'information supplémentaire à insérer.

20 L'addition de l'information supplémentaire au moyen de valeurs de modulation générées par une fonction pseudo aléatoire permet de masquer cette information et de renforcer son invisibilité afin de rendre le piratage de cette information plus difficile.

Selon une version avantageuse de l'invention, à l'étape de choix, 25 le sous-ensemble de composantes est choisi suivant une fonction pseudo aléatoire initialisée par un signal numérique représentatif d'une clé confidentielle associée à l'information supplémentaire à insérer.

Cette clé confidentielle permet de choisir les coefficients modulables de manière pseudo aléatoire et de rendre ainsi l'information insérée 30 plus robuste aux attaques intentionnelles, en rendant sa localisation dans le spectre de fréquence plus difficilement repérable. L'utilisation d'une clé secrète

permet de renforcer la protection du signal inséré dans les données numériques.

Selon un autre aspect de l'invention, un procédé de décodage dans des données numériques marquées d'une information supplémentaire, telle qu'une marque secrète, insérée dans des données numériques initiales selon le
5 procédé d'insertion conforme à l'invention est caractérisé en ce qu'il comporte les étapes suivantes :

- décomposition spectrale multi-résolution des données numériques marquées et des données numériques initiales ;
- 10 - extraction des composantes de plus basse fréquence dans les données numériques marquées et initiales ;
- sélection du sous-ensemble de composantes choisi à l'étape de choix dudit procédé d'insertion dans les données numériques marquées et initiales ;
- 15 - estimation, par soustraction respectivement des composantes dudit sous-ensemble des données numériques marquées et des composantes dudit sous-ensemble des données numériques initiales, d'une séquence estimée de valeurs de modulation ;
- génération d'une séquence présumposée de valeurs de modulation insérées à l'étape de modulation dudit procédé d'insertion ;
- 20 - calcul d'une mesure de corrélation entre la séquence estimée et la séquence présumposée ; et
- décision de la similitude ou non de la séquence estimée et de la séquence présumposée en fonction de ladite mesure de corrélation.

25 Ce procédé de décodage permet ainsi de retrouver aisément les composantes de plus basse fréquence qui ont été modulées pour l'insertion de l'information supplémentaire dans les données numériques et d'estimer la modulation insérée pour la comparer à une modulation présumposée. Un tel procédé de décodage est particulièrement bien adapté à la reconnaissance de
30 droit d'auteurs sur des données numériques qui ont été éventuellement bruitées lors de leur transmission ou stockage.

Corrélativement, un dispositif de décodage dans des données numériques marquées d'une information supplémentaire, telle qu'une marque secrète, insérée dans des données numériques initiales selon le procédé d'insertion conforme à l'invention, est caractérisé en ce qu'il comporte :

- 5 - des moyens de décomposition spectrale multi-résolution des données numériques marquées et des données numériques initiales ;
- des moyens d'extraction des composantes de plus basse fréquence dans les données numériques marquées et initiales ;
- des moyens de sélection du sous-ensemble de composantes
- 10 choisi à l'étape de choix dudit procédé d'insertion dans les données numériques marquées et initiales ;
- des moyens d'estimation, par soustraction respectivement des composantes dudit sous-ensemble des données numériques marquées et des composantes dudit sous-ensemble des données numériques initiales, d'une
- 15 séquence estimée de valeurs de modulation ;
- des moyens de génération d'une séquence présumposée de valeurs de modulation insérées à l'étape de modulation dudit procédé d'insertion ;
- des moyens de calcul d'une mesure de corrélation entre la
- 20 séquence estimée et la séquence présumposée ; et
- des moyens de décision de la similitude ou non de la séquence estimée et de la séquence présumposée en fonction de ladite mesure de corrélation.

25 Ce dispositif de décodage présente des avantages analogues à ceux du procédé de décodage conforme à l'invention et est particulièrement bien adapté à la reconnaissance des droits d'auteur sur des données numériques telles qu'une image numérique par exemple.

30 Selon une version préférée de l'invention, qui permet une réalisation pratique et commode du procédé d'insertion conforme à l'invention, les moyens de décomposition spectrale, d'extraction, de choix, de modulation et de recombposition spectrale du dispositif d'insertion sont incorporés dans :

- un microprocesseur,

- une mémoire morte comportant un programme pour insérer une information supplémentaire, et
- une mémoire vive comportant des registres adaptés à enregistrer des variables modifiées au cours de l'exécution du programme.

5 De manière analogue, et selon une version préférée qui permet une réalisation pratique et commode du procédé de décodage conforme à l'autre aspect de l'invention, les moyens de décomposition spectrale, d'extraction, de sélection, d'estimation, de génération, de calcul et de décision du dispositif de décodage sont incorporés dans :

- 10
- un microprocesseur,
 - une mémoire morte comportant un programme pour décoder une information supplémentaire, et
 - une mémoire vive comportant des registres adaptés à enregistrer des variables modifiées au cours de l'exécution du programme.

15 Un moyen de stockage d'information, lisible par un ordinateur ou par un microprocesseur, intégré ou non au dispositif d'insertion ou de décodage, éventuellement amovible, mémorise un programme mettant en œuvre le procédé d'insertion ou de décodage d'une information supplémentaire conforme à l'invention.

20 La présente invention vise aussi un appareil de traitement de signal numérique comportant des moyens adaptés à mettre en œuvre le procédé d'insertion ou de décodage conforme à l'invention, ou encore comportant un dispositif d'insertion ou de décodage conforme à l'invention.

25 Les avantages de cet appareil de traitement sont identiques à ceux exposés ci-dessus en relation avec le procédé et le dispositif d'insertion conforme à l'invention et le procédé et le dispositif de décodage conforme à l'autre aspect de l'invention.

30 Le procédé d'insertion et le procédé de décodage peuvent plus particulièrement être mis en œuvre dans un appareil photographique numérique, une caméra numérique, un système de gestion de bases de données, un ordinateur, un scanner ou encore un appareillage d'imagerie médicale, et notamment un appareil de radiographie aux rayons X.

Corrélativement, un appareil photographique numérique, une caméra numérique, un système de gestion de bases de données, un ordinateur, un scanner ou un appareillage d'imagerie médicale, et notamment un appareil de radiographie aux rayons X, comportent un dispositif d'insertion et/ou un
5 dispositif de décodage conforme à l'invention.

Ces appareil photographique numérique, caméra numérique, système de gestion de bases de données, ordinateur, scanner et appareillage d'imagerie médicale tel qu'un appareil de radiographie aux rayons X présentent des avantages analogues à ceux des procédés et dispositifs d'insertion et de
10 décodage conformes à l'invention.

D'autres particularités et avantages de l'invention apparaîtront encore dans la description ci-après.

Aux dessins annexés, donnés à titre d'exemples non limitatifs :

- la figure 1 est un schéma de principe illustrant l'insertion d'une
15 information supplémentaire dans un signal numérique ;
- la figure 2 est un diagramme bloc illustrant un dispositif d'insertion conforme à un mode de réalisation de l'invention ;
- la figure 3 est un diagramme bloc illustrant un dispositif de traitement d'un signal numérique adapté à mettre en œuvre le procédé
20 conforme à l'invention ;
- la figure 4 illustre schématiquement un premier mode de décomposition en sous-bande d'une image ;
- la figure 5 illustre schématiquement un second mode de décomposition en sous-bande d'une image ;
- la figure 6 est un algorithme d'insertion d'une information supplémentaire dans une image selon un premier mode de réalisation de
25 l'invention ;
- la figure 7 est un algorithme d'insertion d'une information supplémentaire dans une image selon un second mode de réalisation de
30 l'invention ;
- la figure 8 est un diagramme bloc illustrant un dispositif de décodage conforme à un mode de réalisation de l'invention ;

- la figure 9 est un algorithme de décodage d'une information supplémentaire dans une image selon un premier mode de réalisation de l'invention ; et

5 - la figure 10 est un algorithme de décodage d'une information supplémentaire dans une image selon un second mode de réalisation de l'invention.

On va décrire tout d'abord un dispositif d'insertion d'une information supplémentaire dans des données numériques selon un mode de réalisation de l'invention.

10 Dans l'exemple ci-après, et à titre d'exemple non limitatif, les données numériques sont constituées d'une suite d'échantillons numériques représentant une image I. L'image I est par exemple représentée par une suite d'octets, chaque valeur d'octet représentant un pixel de l'image I, qui peut être une image noir et blanc, à 256 niveaux de gris.

15 L'information supplémentaire est une marque secrète que l'on veut insérer dans l'image I de manière imperceptible et robuste. Cette marque secrète peut par exemple permettre d'identifier le créateur ou propriétaire de l'image I. Cette information supplémentaire se compose dans cet exemple d'un numéro d'identification S sur un certain nombre de bits, par exemple 32 bits,
20 associée à une clé confidentielle K, définie également sur un certain nombre de bits. Ce numéro d'identification S et cette clé confidentielle K permettront de créer, comme décrit ci-après, un signal de modulation qui sera effectivement inséré dans l'image I. La clé confidentielle K peut être associée de manière arbitraire au numéro d'identification S.

25 De manière générale, et comme illustré à la figure 1, un dispositif d'insertion est assimilable globalement à un codeur 1 qui code dans une image I une marque définie à partir de S et K. Une image marquée I' est fournie à la sortie de l'encodeur 1.

30 Cette image I' peut subir un certain nombre de traitements assimilables à l'addition d'un bruit non linéaire, tels qu'une compression et décompression, avec ou sans perte, pour être transmise ou bien stockée, ou

une transformation numérique / analogique pour être visionnée, ou encore un filtrage.

Après traitement, l'image I^* , qui correspond à une version bruitée de l'image marquée I , peut être transmise à un décodeur 2 associé à l'encodeur 1.

- 5 Ce décodeur 2 estimera de manière classique, à partir de l'image originale I et de l'information supplémentaire S , K insérée, le signal de modulation inséré W^* dans l'image bruitée I^* . Ce signal de modulation W^* dans l'image bruitée I^* sera fourni à un détecteur 3, ainsi que le signal de modulation W inséré dans l'image I , afin d'évaluer le taux de similitude entre ces deux signaux W et W^* et de
- 10 vérifier ainsi l'information de droit d'auteur par exemple qui a été insérée. Cette mesure de corrélation sera décrite en détail dans la suite de la description en référence au dispositif et procédé de décodage.

Conformément à l'invention, et comme illustré à la figure 2, le dispositif d'insertion 1 comporte :

- 15 - des moyens de décomposition spectrale multi-résolution 11 des données numériques représentant dans cet exemple une image I ;
- des moyens d'extraction 12 adaptés à extraire des composantes de plus basse fréquence ;
- des moyens de choix 13 pour choisir un sous-ensemble des
- 20 composantes de plus basse fréquence ;
- des moyens de modulation 14 des composantes de ce sous-ensemble pour insérer l'information supplémentaire ; et
- des moyens de recomposition spectrale multi-résolution inverse
- 15 des données numériques afin de reconstituer une image marquée I' .

- 25 De préférence, les moyens de décomposition spectrale multi-résolution 11 sont adaptés à réaliser une décomposition en ondelettes discrète et sont constitués d'un circuit de décomposition en sous-bandes, ou circuit d'analyse, formé d'un ensemble de filtres d'analyse, respectivement associés à des décimateurs par deux. Ce circuit de décomposition filtre le signal d'image I
- 30 selon deux directions, en sous-bandes de basses fréquences et de hautes fréquences spatiales. Le circuit comporte plusieurs blocs successifs d'analyse

pour décomposer l'image I en des sous-bandes selon plusieurs niveaux de résolution.

De manière classique, la résolution d'un signal est le nombre d'échantillons par unité de longueur utilisés pour représenter ce signal. Dans le cas d'un signal image I, la résolution d'une sous-bande est liée au nombre d'échantillons par unité de longueur utilisés pour représenter cette sous-bande. horizontalement et verticalement. La résolution dépend du nombre de décimations effectuées, du facteur de décimation et de la résolution de l'image initiale.

Cette décomposition en sous-bandes est bien connue et nous rappelons ci-dessous brièvement les différentes étapes d'analyse mises en œuvre, en référence à la figure 4, dans le cas d'une image I décomposée en sous-bandes à un niveau de décomposition d égal à 3.

Un premier bloc d'analyse reçoit le signal d'image I et le filtre à travers deux filtres numériques respectivement passe-bas et passe-haut, selon une première direction, par exemple horizontale. Après passage dans des décimateurs par deux, les signaux filtrés résultants sont à leur tour filtrés par deux filtres respectivement passe-bas et passe-haut, selon une seconde direction, par exemple verticale. Chaque signal est à nouveau passé dans un décimateur par deux. On obtient alors en sortie de ce premier bloc d'analyse, quatre sous-bandes LL_1 , LH_1 , HL_1 et HH_1 de résolution la plus élevée dans la décomposition.

La sous-bande LL_1 comporte les composantes de basse fréquence selon les deux directions du signal d'image I. La sous-bande LH_1 comporte les composantes de basse fréquence selon une première direction et de haute fréquence selon une seconde direction du signal image I. La sous-bande HL_1 comporte les composantes de haute fréquence selon la première direction et les composantes de basse fréquence selon la seconde direction. Enfin, la sous-bande HH_1 comporte les composantes de haute fréquence selon les deux directions.

Un second bloc d'analyse filtre à son tour la sous-bande LL_1 pour fournir de la même manière quatre sous-bandes LL_2 , LH_2 , HL_2 et HH_2 de niveau

de résolution intermédiaire dans la décomposition. Enfin, dans cet exemple, la sous-bande LL_2 est à son tour analysée par un troisième bloc d'analyse pour fournir quatre sous-bandes LL_3 , LH_3 , HL_3 et HH_3 de résolution la plus faible dans cette décomposition.

5 On obtient ainsi 10 sous-bandes et trois niveaux de résolution. La sous-bande de plus basse fréquence LL_3 est appelée sous-bande d'approximation et les autres sous-bandes sont des sous-bandes de détail.

Bien entendu, le nombre de niveaux de résolution, et par conséquent de sous-bandes, peut être choisi différemment, et par exemple être égal à
10 quatre niveaux de résolution avec 13 sous-bandes.

Les moyens d'extraction 12 sont ensuite adaptés à choisir les composantes de la sous-bande de plus basse fréquence dans la décomposition de l'image I, c'est-à-dire dans cet exemple la sous-bande d'approximation LL_3 .

L'insertion de la marque S sera ainsi réalisée dans la sous-bande de
15 basse fréquence qui est généralement peu quantifiée dans les traitements de compression et décompression d'image, de sorte que la robustesse de la marque insérée aux distorsions que subit l'image est renforcée.

La Demanderesse a constaté qu'il est possible de rajouter de l'information dans la sous-bande d'approximation de manière imperceptible à
20 condition d'atteindre un niveau de résolution suffisamment faible.

Il convient alors d'ajuster le nombre d de niveaux de décomposition en fonction de la taille de l'image I. En effet, pour une image I de taille N sur N, la sous-bande de très basse fréquence est dans cet exemple de taille $N/2^d \times N/2^d$.

25 De préférence, le nombre d de niveaux de décomposition par la transformation en ondelettes est prédéterminé de telle sorte que le nombre n de composantes de la sous-bande d'approximation LL_d est compris entre 8×8 et 32×32 .

D'après des tests, il s'avère qu'il est préférable d'avoir $n = 16 \times 16$, ce
30 qui correspond à 5 niveaux de décomposition lorsque l'image I a une taille $N \times N = 512 \times 512$.

Les composantes I_{ij} avec $0 \leq i \leq N/2^d - 1$ et $0 \leq j \leq N/2^d - 1$ de la sous-bande d'approximation LL_5 sont ainsi extraites.

A titre de variante, et selon un autre mode de réalisation de la présente invention illustré à la figure 5, les données numériques I sont

5 décomposées de manière itérative en une version d'approximation correspondant à un filtrage passe-bas et un sous-échantillonnage des données numériques I ou d'une version d'approximation précédente, et en une version de détail correspondant à la soustraction de la version d'approximation des données numériques ou de la version d'approximation précédente. Un tel

10 schéma d'approximations successives pyramidal est proposé par Burt et Adelson dans "The laplacian pyramid as a compact image code ", IEEE, Trans. on communications, 31(4) : 532-540, 1983. Ce schéma consiste à extraire une version basse résolution de l'image I considérée par filtrage passe-bas et sous-

15 échantillonnage d'un facteur égal à deux dans chaque direction horizontale et verticale. On obtient ainsi une approximation de niveau 1. L'image de détail de niveau 0, de même taille que l'image d'origine I , est produite par la soustraction de l'approximation de niveau 1 de l'image originale I . Pour effectuer cette soustraction, on prédit dans un premier temps, par interpolation de la version basse résolution, une image de taille identique à l'image originale et on

20 soustrait dans un second temps cette image prédite de l'image originale pour obtenir l'image de détail. Ce schéma peut être itéré autant de fois que nécessaire sur l'image basse résolution pour obtenir une approximation suffisamment simplifiée de l'image et permettre une insertion invisible de l'information supplémentaire dans la version d'approximation. Ici, la

25 décomposition est réitérée sur la version d'approximation de niveau 1 qui est décomposée à son tour en une version d'approximation de niveau 2 et une version de détail de niveau 1. On choisit ensuite à l'étape d'extraction la version de plus basse résolution, ici la version d'approximation de niveau 2, formée également d'un ensemble de composantes I_{ij} , avec i et j variant respectivement

30 sur la longueur de l'image d'approximation de niveau 2 suivant une première et une deuxième direction.

Les moyens de choix 13 d'un sous-ensemble de composantes l_{ij} coopèrent avec un générateur 16 de nombres suivant une fonction pseudo aléatoire initialisée par le signal numérique K représentatif d'une clé confidentielle associée à l'information supplémentaire S à insérer.

5 Le tirage de nombres suivant une fonction pseudo aléatoire permet de renforcer la robustesse de la marque insérée en choisissant les composantes à moduler de manière pseudo aléatoire. Seule la connaissance de la clé confidentielle K et de la fonction pseudo aléatoire utilisée permet de retrouver les composantes de très basse fréquence qui ont été modulées.

10 De même, les moyens de modulation 14 coopèrent avec le générateur 16 de valeurs de modulation générées par une fonction pseudo aléatoire initialisée par un signal numérique S représentatif de l'information supplémentaire à insérer et comportent des moyens d'addition 15 des valeurs de modulation aux composantes du sous-ensemble choisi précédemment.

15 Les moyens de recomposition spectrale 15 comportent un circuit de recomposition classique comprenant une série de filtres de synthèse associés à des multiplicateurs par deux, de sorte qu'après plusieurs niveaux de recomposition, dans cet exemple égal à 3, une image marquée l' est fournie en sortie du codeur 1.

20 De préférence, et comme illustrée à la figure 3, les moyens de décomposition spectrale 11, d'extraction 12, de choix 13, de modulation 14 et de recomposition spectrale 15, ainsi que le générateur 16 de nombres pseudo aléatoires sont incorporés dans un microprocesseur ou ordinateur 10, une mémoire morte 102 (ROM) comportant le programme pour insérer une
25 information supplémentaire S, et une mémoire vive 103 (RAM) comportant des registres adaptés à enregistrer des variables modifiées au cours de l'exécution du programme.

Bien entendu, le programme d'insertion d'une information supplémentaire pourrait être stocké dans un disque dur 108 de l'ordinateur 10.

30 Ce programme d'insertion peut également être mémorisé en totalité ou en partie sur un moyen de stockage qui est amovible et non intégré à l'ordinateur proprement dit. Ainsi, ce programme d'insertion peut être reçu et

chargé dans la mémoire morte 102 ou le disque dur 108 au moyen d'un réseau de communication 113 relié à l'ordinateur par l'intermédiaire d'une interface de communication 112. On peut également envisager que le chargement du programme soit réalisé par l'intermédiaire d'un lecteur de disquettes 109 adapté
5 à lire les instructions de programme préalablement stockées sur une disquette 110. Bien entendu, les disquettes peuvent être remplacées par tout support d'information tel qu'un disque compact à mémoire figée (CD-ROM), une bande magnétique ou encore une carte mémoire.

Une unité centrale 100 (CPU) permet d'exécuter les instructions du
10 programme d'insertion. Ainsi, lors de la mise sous tension, le programme stocké dans une des mémoires non volatiles, par exemple la mémoire morte 102, est transféré dans une mémoire vive (RAM) 103 qui contiendra également les variables nécessaires à la mise en œuvre du procédé d'insertion conforme à l'invention.

15 La mémoire vive 103 peut comporter notamment plusieurs registres pour stocker les variables modifiées au cours de l'exécution du programme. Ainsi, elle comporte à titre d'exemple un registre pour stocker la taille de la sous-bande d'approximation à chaque niveau de décomposition, un registre pour stocker le nombre pseudo aléatoire tiré pour déterminer les composantes
20 à moduler, un registre pour stocker le sous-ensemble de composantes choisi, un registre pour stocker les valeurs de modulation et un registre pour stocker les composantes modulées.

Un bus de communication 101 permet de manière classique la communication entre les différents sous-éléments de l'ordinateur.

25 L'ordinateur 10 possède en outre un écran 104 permettant de visualiser par exemple l'image I à marquer et de servir d'interface avec l'utilisateur qui pourra paramétrer certaines données pour la mise en œuvre du procédé d'insertion, à l'aide du clavier 114 par exemple.

La fourniture des données, dans lesquelles on souhaite insérer une
30 marque secrète, par exemple pour identifier leur auteur, à l'ordinateur 10 peut être réalisée par différents périphériques et notamment une caméra numérique 107 reliée à une carte graphique, ou encore un scanner, un appareil de

radiographie aux rayons X ou tout autre moyen d'acquisition ou de stockage d'images.

Le réseau de communication 113 peut également être adapté à fournir une image numérique à marquer. La disquette 110 peut de même
5 contenir des données numériques.

A titre de variante, un microphone 111 est relié à l'ordinateur 10 par l'intermédiaire d'une carte entrée-sortie 106. Les données numériques à marquer seront dans cette variante un signal audio.

Ce dispositif d'insertion peut également être incorporé dans tout type
10 d'appareil de traitement numérique, directement dans un appareil photographique numérique ou une caméra numérique, ou encore être intégré à un système de gestion de bases de données pour marquer les données numériques mémorisées ou traitées.

On va décrire maintenant le procédé d'insertion conforme à
15 l'invention en référence notamment aux figures 6 et 7.

Selon l'invention, le procédé d'insertion d'une information supplémentaire S, telle qu'une marque secrète, dans des données numériques, ici une image I, comporte les étapes suivantes :

a) décomposition spectrale multi-résolution E1 des données
20 numériques I ;

b) extraction E2 des composantes de plus basse fréquence.

On applique ici, à titre d'exemple, le procédé d'insertion à une image I de taille N sur N avec $N = 512$ octets.

La décomposition spectrale E1 est réalisée dans le mode de
25 réalisation de la figure 6 par une transformation en ondelettes discrète. Le nombre d de niveaux de décomposition par la transformation en ondelettes est prédéterminé de telle sorte que le nombre n de composantes de la sous-bande d'approximation LL est compris entre 8×8 et 32×32 .

On fixe ainsi une valeur de seuil T, par exemple 32×32 , et l'on
30 compare à chaque niveau de décomposition, le nombre n de composantes de la sous-bande d'approximation LL à cette valeur de seuil T lors d'une étape de test E21.

Si le test est négatif, c'est à dire que n est supérieur à la valeur de seuil T , on décompose la sous-bande à un niveau de décomposition supérieur.

Dans cet exemple, où l'image I est carrée et de taille égale à 512x512 octets, on utilise une décomposition en sous-bandes avec des
5 décimateurs par deux. La taille de la sous-bande LL , également carrée, est, à chaque niveau d de décomposition, égale à $N/2^d \times N/2^d$.

En fixant une valeur de seuil T à 32x32, on obtient une sous-bande LL de taille adéquate pour un niveau de décomposition d égal à 4.

A l'étape $E2$, on choisit par conséquent la sous-bande
10 d'approximation LL_4 de plus basse fréquence formée des composantes I_{ij} , avec $0 \leq i \leq N/2^d - 1$ et $0 \leq j \leq N/2^d - 1$.

Alternativement, dans le mode de réalisation illustré à la figure 7, on décompose le signal image I par une décomposition de type pyramidal comme décrit ci-dessus en référence à la figure 5. A chaque niveau de décomposition,
15 on compare, à l'étape $E21$, le nombre n de composantes de l'approximation obtenue à la valeur de seuil T , fixée par exemple à 32x32, afin de déterminer de la même manière que pour la décomposition en ondelettes discrète si la taille de l'approximation est suffisamment faible ou si la décomposition doit être réitérée à un niveau supérieur.

Dans une étape $E3$, on procède conformément à l'invention au choix
20 d'un sous-ensemble de composantes I_{ij} de la sous-bande de très basse fréquence extraite. Les composantes à moduler sont ainsi choisies dans un domaine spectral restreint.

Dans ces exemples de réalisation, on se fixe pour la modulation un
25 taux de couverture de $x\%$ de la sous-bande de très basse fréquence extraite. Par exemple, on choisit $x = 80$.

Dans cet exemple, le sous-ensemble de composantes est choisi suivant une fonction pseudo aléatoire initialisée par un signal numérique K représentatif d'une clé confidentielle associée à l'information supplémentaire S
30 à insérer.

On définit un ordre de balayage des composantes I_{ij} . Lorsque ces composantes sont en matrice de dimension $N/2^d \times N/2^d$, on choisit par exemple

l'ordre de balayage vidéo, en zigzag du coin supérieur gauche au coin inférieur droit.

Pour chaque composante l_{ij} , on fait un tirage à l'étape E31 selon une loi uniforme U prédéterminée, telle qu'une loi uniforme U sur l'intervalle $[0,1]$,
5 initialisée par K , de telle sorte que l'on obtient un nombre pseudo aléatoire $b_k = U(K)$ compris entre 0 et 1.

De manière connue, une loi uniforme U sur cet intervalle est constituée d'une suite de nombres réels, uniformément répartis sur l'intervalle $]0,1]$, chaque nombre de l'intervalle ayant la même probabilité d'occurrence. A
10 chaque valeur d'initialisation K correspond une suite donnée de nombres réels : cette valeur d'initialisation K peut être assimilée à une clé secrète dont la connaissance permet de reconstituer à l'identique la suite de nombres réels.

A chaque tirage de b_k , c'est-à-dire pour chaque valeur successive de la suite de nombres réels définis par la loi uniforme U , on compare ce nombre
15 b_k au taux de couverture $x/100$ dans une étape de test E32. Si b_k est inférieur à $x/100$, ici égal à 0,8, la composante l_{ij} associée est retenue pour être modulée. A contrario, si le nombre b_k est supérieur à 0,8, la composante l_{ij} associée est maintenue inchangée et réinsérée dans la sous-bande de très basse fréquence à une étape E33.

20 Dans cet exemple particulier, la proportion de composantes l_{ij} qui sont modulées est égale statistiquement à quatre cinquièmes des composantes de très basse fréquence extraites à l'étape E2.

Bien entendu, sans clé confidentielle K , le choix des composantes à moduler peut être fait de façon systématique par exemple en choisissant quatre
25 coefficients sur cinq dans l'ordre de parcours. On peut également choisir les plus gros coefficients en magnitude ou encore les premiers coefficients dans l'ordre de parcours en zigzag de la sous-bande de très basse fréquence.

Toujours selon l'invention, les composantes l_{ij} du sous-ensemble choisi sont modulées à l'étape E4 par addition d'une valeur de modulation
30 générée par une fonction pseudo aléatoire dans une étape E41 initialisée par le signal numérique S représentatif de l'information supplémentaire à insérer.

On utilise à titre d'exemple une loi Gaussienne $G(0,1)$ initialisée dans le générateur 16 de nombre pseudo aléatoire par le signal à insérer S .

On effectue à l'étape E41 un tirage d'une valeur de modulation $w_k = G(S)$ pour chaque composante l_{ij} à moduler, l'indice k correspondant à la $k^{\text{ième}}$ composante l_{ij} à moduler dans l'ordre de balayage prédéfini. A chaque signal d'initialisation S correspond une suite unique prédéterminée de valeurs de modulation w_k de moyenne égale à 0 et d'écart-type égal à 1.

Un coefficient de correction α est calculé à l'étape E42. Ce coefficient α peut être constant pour toutes les composantes l_{ij} à moduler et être typiquement égal à 1. Il permet d'assurer l'invisibilité de l'information insérée S .

La modulation de chaque composante l_{ij} est obtenue par addition à l'étape E4 de la valeur de modulation :

$$l'_{ij} = l_{ij} + \alpha w_k$$

Le choix d'un coefficient de correction α constant est suffisant dans ces exemples de réalisation utilisant une décomposition en ondelettes ou une décomposition de type pyramidal, étant donné que les composantes l_{ij} ont des ordres de grandeur comparables.

Le coefficient de correction α pourrait également être dépendant des composantes l_{ij} , de telle sorte que la modulation de chaque composante l_{ij} est obtenue par addition à l'étape E4 de la valeur de modulation :

$$l'_{ij} = l_{ij} + \alpha_{ij} w_k$$

Le coefficient α_{ij} peut être pondéré en fonction de la valeur de la composante modulée de sorte que $\alpha_{ij} = 0,1 \times l_{ij}$.

Le coefficient α_{ij} peut correspondre également à la moyenne des valeurs l_{ij} du voisinage de la composante modulée.

Il peut également tenir compte de la limite de visibilité locale afin d'assurer un masquage psychovisuel de sorte que la modulation des composantes pour l'insertion de la marque secrète ne dépasse pas la distorsion maximale acceptable visuellement.

Les composantes modulées l'_{ij} sont ensuite réinsérées à l'étape E33 dans les composantes de très basse fréquence à la place des composantes initiales l_{ij} .

Un test est effectué à l'étape E34 pour vérifier si toutes les composantes I_{ij} de très basse fréquence ont été balayées.

Dans la négative, on considère la composante I_{ij} suivante dans l'ordre de balayage et on réitère le procédé à partir de l'étape E3 par tirage d'un
5 nouveau nombre pseudo aléatoire b_k pour déterminer si cette composante I_{ij} doit être modulée.

Lorsque le balayage est terminé, une dernière étape de recomposition spectrale multi-résolution inverse E5 permet de reconstruire l'image marquée I' .

10 Dans l'exemple de réalisation de la figure 6, on utilise des filtres de synthèse pour mettre en œuvre une transformation en ondelettes inverse.

Dans l'exemple de la figure 7, on reconstruit l'image marquée I' à partir des versions d'approximations et de détails successives.

Grâce au procédé d'insertion conforme à l'invention, la marque
15 insérée S dans l'image I' est bien plus robuste aux traitements ultérieurs de l'image I' . En outre, la modulation insérée est limitée à une bande de fréquences et la vérification de la marque insérée sera plus rapide à effectuer.

Le décodage d'une marque insérée va maintenant être décrit en référence plus particulièrement aux figures 8 à 10.

20 Le décodeur 2 (voir figure 1) reçoit une image bruitée I^* et il dispose également de l'image originale I ainsi que de l'information S associée à la clé confidentielle K .

Comme illustré à la figure 8, le dispositif de décodage conforme à l'invention comporte :

- 25
- des moyens de décomposition spectrale multi-résolution 61 des données numériques marquées I^* et des données numériques initiales I ;
 - des moyens d'extraction 62 des composantes de plus basse fréquence dans les données numériques marquées I^* et initiales I ;
 - des moyens de sélection 63 du sous-ensemble de composantes
- 30 choisi à l'étape de choix E3 du procédé d'insertion précédemment décrit dans les données numériques marquées I^* et initiales I ;

- des moyens d'estimation 64 par soustraction respectivement des composantes l_{ij}^* dudit sous-ensemble des données numériques marquées l^* et des composantes l_{ij} dudit sous-ensemble des données numériques initiales l , d'une séquence estimée W^* de valeurs de modulation w_k^* ;

5 - des moyens de génération 65 d'une séquence présumposée W de valeurs de modulation w_k insérées à l'étape de modulation E4 dudit procédé d'insertion ;

- des moyens de calcul d'une mesure de corrélation entre la séquence estimée W^* et la séquence présumposée W ; et

10 - des moyens de décision 68 de la similitude ou non de la séquence estimée W^* et de la séquence présumposée W en fonction de ladite mesure de corrélation.

De manière analogue au dispositif d'insertion, les moyens de décomposition spectrale 61 peuvent être adaptés à réaliser une transformation en ondelettes discrète, les moyens d'extraction 62 étant adaptés à choisir les composantes de la sous-bande d'approximation LL. Cette décomposition spectrale a été décrite en détails ci-dessus.

Dans un second mode de réalisation de l'invention, les moyens de décomposition spectrale 61 sont adaptés à décomposer les données numériques initiales l et marquées l^* de manière itérative en une version d'approximation correspondant à un filtrage passe-bas et un sous-échantillonnage des données numériques ou d'une version d'approximation précédente, et en une version de détail correspondant à la soustraction de la version d'approximation des données numériques ou de ladite version d'approximation précédente, les moyens d'extraction 62 étant adaptés à choisir les composantes de la version d'approximation.

On comprendra aisément que le choix de ces moyens de décomposition spectrale dépend du type de décomposition utilisée lors de l'insertion de l'information secrète S .

30 Les moyens de génération 65 de la séquence présumposée W de valeurs de modulation coopèrent avec un générateur 66 de valeurs de

modulation générées par une fonction pseudo aléatoire initialisée par un signal numérique S représentatif de l'information supplémentaire à décoder.

5 Ce générateur 66 est identique au générateur 16 utilisé dans le dispositif d'insertion et permet de recalculer les valeurs de modulation w_k en utilisant la même loi Gaussienne G initialisée par le signal numérique S représentatif de l'information supplémentaire que l'on souhaite décoder.

De même, les moyens de sélection 63 coopèrent avec un générateur 66 de nombres b_k suivant une fonction pseudo aléatoire initialisée par un signal numérique K représentatif d'une clé confidentielle associée à l'information
10 supplémentaire S à décoder.

Comme illustré à la figure 3, les moyens de décomposition spectrale 61, d'extraction 62, de sélection 63, d'estimation 64, de génération 65, de calcul 67 et de décision 68 sont incorporés dans un microprocesseur 10, une mémoire morte 102 comportant un programme pour décoder une information
15 supplémentaire S et une mémoire vive 103 comportant des registres adaptés à enregistrer des variables modifiées au cours de l'exécution du programme.

Le microprocesseur 10 et son fonctionnement sont identiques à ceux décrits précédemment pour le dispositif et le procédé d'insertion.

Le programme de décodage d'une information supplémentaire
20 pourrait être stocké dans un disque dur 108 de l'ordinateur 10 ou être mémorisé en totalité ou en partie sur un moyen de stockage qui est amovible et non intégré à l'ordinateur proprement dit.

Une unité centrale 100 (CPU) permet d'exécuter les instructions du programme de décodage. Ainsi, lors de la mise sous tension, le programme
25 stocké dans une des mémoires non volatiles, par exemple la mémoire morte 102, est transféré dans une mémoire vive (RAM) 103 qui contiendra également les variables nécessaires à la mise en œuvre du procédé de décodage conforme à l'invention.

La mémoire vive 103 peut comporter notamment plusieurs registres
30 pour stocker les variables modifiées au cours de l'exécution du programme. Ainsi, elle comporte à titre d'exemple un registre pour stocker la taille de la sous-bande d'approximation à chaque niveau de décomposition, un registre

pour stocker le nombre pseudo aléatoire tiré pour déterminer les composantes à moduler, un registre pour stocker le sous-ensemble de composantes choisi, un registre pour stocker la séquence estimée de valeurs de modulation, un registre pour stocker la séquence présumée de valeurs de modulation et un
5 registre pour stocker le calcul de la mesure de corrélation.

La fourniture des données, dans lesquelles on souhaite décoder une marque secrète, par exemple pour identifier leur auteur, à l'ordinateur 10 peut être réalisée par différents périphériques et notamment une caméra numérique 107 reliée à une carte graphique, ou encore un scanner, un appareil de radiographie aux rayons X ou tout autre moyen d'acquisition ou de stockage d'images.

Le réseau de communication 113 peut également être adapté à fournir une image numérique à décoder. La disquette 110 peut de même contenir des données numériques.

15 Ce dispositif de décodage peut également être incorporé dans tout type d'appareil de traitement numérique, directement dans un appareil photographique numérique ou une caméra numérique, ou encore être intégré à un système de gestion de bases de données pour décoder les données numériques mémorisées ou traitées.

20 On va décrire à présent de manière plus détaillée le procédé de décodage conforme à l'invention permettant de décoder une information supplémentaire S insérée dans des données numériques I selon le procédé d'insertion conforme à l'invention.

Ce procédé de décodage comporte en référence aux figures 9 et 10
25 les étapes suivantes :

- décomposition spectrale multi-résolution E6 des données numériques marquées I* et des données numériques initiales I ;
- extraction E7 des composantes de plus basse fréquence dans les données numériques marquées I* et initiales I ;
- 30 - sélection E8 du sous-ensemble de composantes choisi à l'étape de choix E3 dudit procédé d'insertion dans les données numériques marquées I* et initiales I ;

- estimation E9, par soustraction respectivement des composantes dudit sous-ensemble des données numériques marquées I^* et des composantes dudit sous-ensemble des données numériques initiales I d'une séquence estimée W^* de valeurs de modulation ;
- 5 - génération E10 d'une séquence présumée W de valeurs de modulation insérées à l'étape de modulation E4 dudit procédé d'insertion ;
- calcul E11 d'une mesure de corrélation entre la séquence estimée W^* et la séquence présumée W ; et
- décision E12 de la similitude ou non de la séquence estimée W^*
- 10 et de la séquence présumée W en fonction de ladite mesure de corrélation.

Les figures 9 et 10 illustrent des procédés de décodage identiques hormis dans leurs étapes de décomposition E6 et d'extraction E7.

Dans un premier mode de réalisation illustré à la figure 9, la décomposition spectrale est réalisée par une transformation en ondelettes discrète, et à l'étape d'extraction E7, on choisit les composantes de la sous-

15 bande d'approximation LL.

Un tel procédé de décodage est mis en œuvre lorsque l'information supplémentaire S a été insérée suivant un procédé d'insertion conforme au premier mode de réalisation de l'invention décrit en référence à la figure 6.

20 Dans un second mode de réalisation du procédé de décodage, illustré à la figure 10, lors de la décomposition spectrale E6, les données numériques initiales I et marquées I^* sont décomposées de manière itérative en une version d'approximation correspondant à un filtrage passe-bas et un sous-échantillonnage des données numériques ou d'une version d'approximation

25 précédente, et en une version de détail correspondant à la soustraction de la version d'approximation des données numériques ou de ladite version d'approximation précédente, et à l'étape d'extraction E7, on choisit les composantes de la version d'approximation.

Un tel procédé de décodage est mis en œuvre lorsque l'information

30 supplémentaire S a été insérée suivant un procédé d'insertion conforme à un second mode de réalisation du procédé d'insertion tel que décrit en référence à la figure 7.

Dans les deux cas, les méthodes de décomposition spectrale multi-résolution sont identiques à celles mises en œuvre dans le procédé d'insertion associé.

5 A chaque niveau de décomposition, on vérifie dans une étape de test E71, si la taille de la sous-bande d'approximation est inférieure à une valeur de seuil T, et dans la négative, on réitère la décomposition spectrale à un niveau de décomposition supérieur. La valeur de seuil utilisée T est identique à celle utilisée dans le procédé d'insertion décrit ci-dessus.

10 A l'étape de sélection E8, le sous-ensemble de composantes est choisi suivant une fonction pseudo aléatoire initialisée par un signal numérique K représentatif d'une clé confidentielle associée à l'information supplémentaire S à décoder.

15 On utilise une loi uniforme U identique à celle utilisée lors du procédé d'insertion et initialisée par la clé confidentielle K afin de retrouver la même suite de nombres réels pseudo aléatoires. On peut ainsi retrouver l'ensemble des composantes l_{ij}^* modulées dans l'image bruitée l^* et les composantes initiales l_{ij} qui ont été modulées.

20 Pour chaque composante l_{ij} et l_{ij}^* prise dans un ordre de balayage prédéterminé des sous-bandes d'approximation LL des données numériques initiales l et marquées l^* , on effectue, dans une étape E81, un tirage de $b_k = U(K)$. On compare, à une étape E82, ce nombre b_k à un taux de couverture $x/100$, ici égal à 0,8.

Si b_k est supérieur à 0,8, on passe directement à la composante suivante dans l'ordre de balayage prédéfini.

25 Sinon, on effectue à l'étape E9, la différence entre les composantes l_{ij} et l_{ij}^* pour obtenir une estimation w_k^* des valeurs de modulation insérée w_k pour chaque composante modulée :

$$w_k^* = \frac{1}{\alpha} (l_{ij}^* - l_{ij})$$

30 On teste, dans une étape E83 si le balayage des sous-bandes LL est terminé. Dans la négative, on réitère les étapes E8 et suivantes pour les composantes suivantes dans l'ordre de balayage.

On obtient ainsi une séquence W^* correspondant à la suite des valeurs estimées w_k^* .

Le décodeur dispose également de l'information S et peut calculer dans une étape de génération E10 la séquence présumée W des valeurs de modulation w_k , c'est-à-dire l'ensemble des w_k suivant la loi Gaussienne $G(S)$ utilisée lors de l'étape de modulation E4 du procédé d'insertion.

On effectue alors dans une étape de calcul E11 une mesure de corrélation entre W et W^* , par exemple en utilisant une mesure de corrélation normalisée :

$$10 \quad \text{corr}(W, W^*) = \frac{(W, W^*)}{\|W\| \times \|W^*\|}$$

$$\text{où } (W, W^*) = \sum_k w_k w_k^* \text{ et } \|W\| = \sqrt{(W, W)}.$$

Le calcul d'un taux de ressemblance par $100 \times \text{corr}(W, W^*)$ permet de décider dans une étape de décision E12 de la similitude ou non des deux séquences W et W^* .

15 Au-dessus de 50%, la corrélation est considérée suffisante pour donner une réponse positive en sortie du détecteur 3. Bien entendu, plus la corrélation est proche de 100%, plus la détection et donc la reconnaissance d'une information insérée S est fiable.

20 On constate ici que le procédé d'insertion conforme à l'invention donne lors du décodage un taux de ressemblance supérieur à 75% pour divers algorithmes de compression tel que JPEG (Joint Photographic Expert Group) jusqu'à un facteur de qualité de 5, ce qui correspond à une image fortement dégradée.

25 Le procédé d'insertion conforme à l'invention et le dispositif associé permettent ainsi d'accroître fortement la robustesse d'une information insérée dans des données numériques de manière imperceptible.

Bien entendu, l'invention n'est pas limitée aux exemples décrits ci-dessus, et de nombreuses modifications peuvent être apportées à celui-ci sans sortir du cadre de l'invention.

30 Ainsi, les données numériques marquées pourraient également être des données audio.

REVENDEICATIONS

1. Procédé d'insertion d'une information supplémentaire (S), telle qu'une marque secrète, dans des données numériques (I), caractérisé en ce
5 qu'il comporte les étapes suivantes :

- décomposition spectrale multi-résolution (E1) des données numériques (I) ;
- extraction (E2) des composantes de plus basse fréquence ;
- choix (E3) d'un sous-ensemble des composantes de plus basse
10 fréquence ;
- modulation (E4) des composantes dudit sous-ensemble pour insérer l'information supplémentaire (S) ; et
- recombinaison spectrale multi-résolution inverse (E5) des données numériques marquées (I').

15 2. Procédé d'insertion conforme à la revendication 1, caractérisé en ce que le niveau (d) de décomposition spectrale multi-résolution est prédéterminé de telle sorte que le nombre (n) de composantes de plus basse fréquence est compris entre 8x8 et 32x32.

3. Procédé d'insertion conforme à l'une des revendications 1 ou 2, caractérisé en ce qu'à l'étape de décomposition spectrale (E1), la
20 décomposition spectrale est réalisée par une transformation en ondelettes discrète, et à l'étape d'extraction (E2), on choisit les composantes de la sous-bande d'approximation (LL).

4. Procédé d'insertion conforme à l'une des revendications 1 ou 2, caractérisé en ce qu'à l'étape de décomposition spectrale (E1), les données
25 numériques (I) sont décomposées de manière itérative en une version d'approximation correspondant à un filtrage passe-bas et un sous-échantillonnage des données numériques ou d'une version d'approximation précédente, et en une version de détail correspondant à la soustraction de la
30 version d'approximation des données numériques ou de ladite version d'approximation précédente, et en ce qu'à l'étape d'extraction (E2), on choisit les composantes de la version d'approximation.

5. Procédé d'insertion conforme à l'une des revendications 1 à 4, caractérisé en ce qu'à l'étape de modulation (E4), les composantes dudit sous-ensemble sont modulées par addition d'une valeur de modulation (w_k) générée par une fonction pseudo aléatoire initialisée par un signal numérique (S) représentatif de l'information supplémentaire à insérer.

6. Procédé d'insertion conforme à l'une des revendications 1 à 5, caractérisé en ce qu'à l'étape de choix (E3), le sous-ensemble de composantes est choisi suivant une fonction pseudo aléatoire initialisée par un signal numérique (K) représentatif d'une clé confidentielle associée à l'information supplémentaire (S) à insérer.

7. Dispositif d'insertion d'une information supplémentaire (S), telle qu'une marque secrète, dans des données numériques (I), caractérisé en ce qu'il comporte :

- des moyens de décomposition spectrale multi-résolution (11) des données numériques (I) ;
- des moyens d'extraction (12) adaptés à extraire des composantes de plus basse fréquence ;
- des moyens de choix (13) pour choisir un sous-ensemble des composantes de plus basse fréquence ;
- des moyens de modulation (14) des composantes dudit sous-ensemble pour insérer l'information supplémentaire (S) ; et
- des moyens de recomposition spectrale multi-résolution inverse (15) des données numériques marquées (I').

8. Dispositif d'insertion conforme à la revendication 7, caractérisé en ce que le niveau (d) de décomposition spectrale multi-résolution est prédéterminé de telle sorte que le nombre (n) de composantes de plus basse fréquence est compris entre 8×8 et 32×32 .

9. Dispositif d'insertion conforme à l'une des revendications 7 ou 8, caractérisé en ce que les moyens de décomposition spectrale multi-résolution (11) sont adaptés à réaliser une transformation en ondelettes discrète, les moyens d'extraction (12) étant adaptés à choisir les composantes de la sous-bande d'approximation (LL).

10. Dispositif d'insertion conforme à l'une des revendications 7 ou 8, caractérisé en ce que les moyens de décomposition spectrale multi-résolution (11) sont adaptés à décomposer les données numériques (I) de manière itérative en une version d'approximation correspondant à un filtrage passe-bas
5 et un sous-échantillonnage des données numériques ou d'une version d'approximation précédente, et en une version de détail correspondant à la soustraction de la version d'approximation des données numériques ou de ladite version d'approximation précédente, les moyens d'extraction (12) étant adaptés à choisir les composantes de la version d'approximation.

10 11. Dispositif d'insertion conforme à l'une des revendications 7 à 10, caractérisé en ce que les moyens de modulation (14) coopèrent avec un générateur (16) de valeurs de modulation (w_k) générées par une fonction pseudo aléatoire initialisée par un signal numérique (S) représentatif de l'information supplémentaire à insérer et comportent des moyens d'addition (15)
15 des valeurs de modulation (w_k) aux composantes dudit sous-ensemble.

12. Dispositif d'insertion conforme à l'une des revendications 7 à 11, caractérisé en ce que les moyens de choix (13) pour choisir un sous-ensemble de composantes coopèrent avec un générateur (16) de nombres (b_k) suivant une fonction pseudo aléatoire initialisée par un signal numérique (K)
20 représentatif d'une clé confidentielle associée à l'information supplémentaire (S) à insérer.

13. Dispositif d'insertion conforme à l'une des revendications 7 à 12, caractérisé en ce que les moyens de décomposition spectrale (11), d'extraction (12), de choix (13), de modulation (14) et de recomposition spectrale (15) sont
25 incorporés dans :

- un microprocesseur (10) ;
- une mémoire morte (102) comportant un programme pour insérer une information supplémentaire (S) ; et
- une mémoire vive (103) comportant des registres adaptés à
30 enregistrer des variables modifiées au cours de l'exécution du programme.

14. Procédé de décodage dans des données numériques marquées (I^*) d'une information supplémentaire (S), telle qu'une marque secrète, insérée

dans des données numériques initiales (I) selon le procédé d'insertion conforme à l'une des revendications 1 à 6, caractérisé en ce qu'il comporte les étapes suivantes :

- décomposition spectrale multi-résolution (E6) des données numériques marquées (I*) et des données numériques initiales (I) ;
- extraction (E7) des composantes de plus basse fréquence dans les données numériques marquées (I*) et initiales (I) ;
- sélection (E8) du sous-ensemble de composantes choisi à l'étape de choix (E3) dudit procédé d'insertion dans les données numériques marquées (I*) et initiales (I) ;
- estimation (E9), par soustraction respectivement des composantes dudit sous-ensemble des données numériques marquées (I*) et des composantes dudit sous-ensemble des données numériques initiales (I), d'une séquence estimée (W*) de valeurs de modulation ;
- génération (E10) d'une séquence présumposée (W) de valeurs de modulation insérées à l'étape de modulation (E4) dudit procédé d'insertion ;
- calcul (E11) d'une mesure de corrélation entre la séquence estimée (W*) et la séquence présumposée (W) ;
- décision (E12) de la similitude ou non de la séquence estimée (W*) et de la séquence présumposée (W) en fonction de ladite mesure de corrélation.

15. Procédé de décodage conforme à la revendication 14, caractérisé en ce qu'à l'étape de décomposition spectrale (E6), la décomposition spectrale est réalisée par une transformation en ondelettes discrète, et à l'étape d'extraction (E7), on choisit les composantes de la sous-bande d'approximation (LL).

16. Procédé de décodage conforme à la revendication 14, caractérisé en ce qu'à l'étape de décomposition spectrale (E6), les données numériques initiales (I) et marquées (I*) sont décomposées de manière itérative en une version d'approximation correspondant à un filtrage passe-bas et un sous-échantillonnage des données numériques ou d'une version d'approximation précédente, et en une version de détail correspondant à la

soustraction de la version d'approximation des données numériques ou de ladite version d'approximation précédente, et en ce qu'à l'étape d'extraction (E7), on choisit les composantes de la version d'approximation.

5 17. Procédé de décodage conforme à l'une des revendications 14 à 16, caractérisé en ce qu'à l'étape de génération (E10), la séquence présumée (W) de valeurs de modulation est générée par une fonction pseudo aléatoire initialisée par un signal numérique (S) représentatif de l'information supplémentaire à décoder.

10 18. Procédé de décodage conforme à l'une des revendications 14 à 17, caractérisé en ce qu'à l'étape de sélection (E8), le sous-ensemble de composantes est choisi suivant une fonction pseudo aléatoire initialisée par un signal numérique (K) représentatif d'une clé confidentielle associée à l'information supplémentaire (S) à décoder.

15 19. Dispositif de décodage dans des données numériques marquées (I*) d'une information supplémentaire (S), telle qu'une marque secrète, insérée dans des données numériques initiales (I) selon le procédé d'insertion conforme à l'une des revendications 1 à 6, caractérisé en ce qu'il comporte :

- des moyens de décomposition spectrale multi-résolution (61) des données numériques marquées (I*) et des données numériques initiales (I) ;
- 20 - des moyens d'extraction (62) des composantes de plus basse fréquence dans les données numériques marquées (I*) et initiales (I) ;
- des moyens de sélection (63) du sous-ensemble de composantes choisi à l'étape de choix (E3) dudit procédé d'insertion dans les données numériques marquées (I*) et initiales (I) ;
- 25 - des moyens d'estimation (64), par soustraction respectivement des composantes dudit sous-ensemble des données numériques marquées (I*) et des composantes dudit sous-ensemble des données numériques initiales (I) d'une séquence estimée (W*) de valeurs de modulation ;
- des moyens de génération (65) d'une séquence présumée (W)
- 30 de valeurs de modulation insérées à l'étape de modulation (E4) dudit procédé d'insertion ;

- des moyens de calcul (67) d'une mesure de corrélation entre la séquence estimée (W^*) et la séquence présumée (W) ; et

- des moyens de décision (68) de la similitude ou non de la séquence estimée (W^*) et de la séquence présumée (W) en fonction de ladite mesure de corrélation.

20. Dispositif de décodage conforme à la revendication 19, caractérisé en ce que les moyens de décomposition spectrale (61) sont adaptés à réaliser une transformation en ondelettes discrète, les moyens d'extraction (62) étant adaptés à choisir les composantes de la sous-bande d'approximation (LL).

21. Dispositif de décodage conforme à la revendication 19, caractérisé en ce que les moyens de décomposition spectrale (61) sont adaptés à décomposer les données numériques initiales (I) et marquées (I^*) de manière itérative en une version d'approximation correspondant à un filtrage passe-bas et un sous-échantillonnage des données numériques ou d'une version d'approximation précédente, et en une version de détail correspondant à la soustraction de la version d'approximation des données numériques ou de ladite version d'approximation précédente, les moyens d'extraction (62) étant adaptés à choisir les composantes de la version d'approximation.

22. Dispositif de décodage conforme à l'une des revendications 19 à 21, caractérisé en ce que les moyens de génération (65) de la séquence présumée (W) de valeurs de modulation coopèrent avec un générateur (66) de valeurs de modulation générées par une fonction pseudo aléatoire initialisée par un signal numérique (S) représentatif de l'information supplémentaire à décoder.

23. Dispositif de décodage conforme à l'une des revendications 19 à 22, caractérisé en ce que les moyens de sélection (63) coopèrent avec un générateur (66) de nombres (b_k) suivant une fonction pseudo aléatoire initialisée par un signal numérique (K) représentatif d'une clé confidentielle associée à l'information supplémentaire (S) à décoder.

24. Dispositif de décodage conforme à l'une des revendications 19 à 23, caractérisé en ce que les moyens de décomposition spectrale (61),

d'extraction (62), de sélection (63), d'estimation (64), de génération (65), de calcul (67) et de décision (68) sont incorporés dans :

- un microprocesseur (10) ;
- une mémoire morte (102) comportant un programme pour
5 décoder une information supplémentaire (S) ; et
- une mémoire vive (103) comportant des registres adaptés à enregistrer des variables modifiées au cours de l'exécution du programme.

25. Appareil de traitement de signal numérique, caractérisé en ce qu'il comporte des moyens adaptés à mettre en œuvre le procédé d'insertion
10 conforme à l'une des revendications 1 à 6.

26. Appareil de traitement de signal numérique, caractérisé en ce qu'il comporte un dispositif d'insertion conforme à l'une des revendications 7 à 13.

27. Appareil de traitement de signal numérique, caractérisé en ce
15 qu'il comporte des moyens adaptés à mettre en œuvre le procédé de décodage conforme à l'une des revendications 14 à 18.

28. Appareil de traitement de signal numérique, caractérisé en ce qu'il comporte un dispositif de décodage conforme à l'une des revendications 19 à 24.

29. Appareil photographique numérique, caractérisé en ce qu'il
20 comporte des moyens adaptés à mettre en œuvre le procédé d'insertion conforme à l'une des revendications 1 à 6.

30. Appareil photographique numérique, caractérisé en ce qu'il comporte un dispositif d'insertion conforme à l'une des revendications 7 à 13.

31. Appareil photographique numérique, caractérisé en ce qu'il
25 comporte des moyens adaptés à mettre en œuvre le procédé de décodage conforme à l'une des revendications 14 à 18.

32. Appareil photographique numérique, caractérisé en ce qu'il
30 comporte un dispositif de décodage conforme à l'une des revendications 19 à 24.

33. Caméra numérique, caractérisée en ce qu'elle comporte des moyens adaptés à mettre en œuvre le procédé d'insertion conforme à l'une des revendications 1 à 6.

5 34. Caméra numérique, caractérisée en ce qu'elle comporte un dispositif d'insertion conforme à l'une des revendications 7 à 13.

35. Caméra numérique, caractérisée en ce qu'elle comporte des moyens adaptés à mettre en œuvre le procédé de décodage conforme à l'une des revendications 14 à 18.

10 36. Caméra numérique, caractérisée en ce qu'elle comporte un dispositif de décodage conforme à l'une des revendications 19 à 24.

37. Système de gestion de bases de données, caractérisé en ce qu'il comporte des moyens adaptés à mettre en œuvre le procédé d'insertion conforme à l'une des revendications 1 à 6.

15 38. Système de gestion de bases de données, caractérisé en ce qu'il comporte un dispositif d'insertion conforme à l'une des revendications 7 à 13.

39. Système de gestion de bases de données, caractérisé en ce qu'il comporte des moyens adaptés à mettre en œuvre le procédé de décodage conforme à l'une des revendications 14 à 18.

20 40. Système de gestion de bases de données, caractérisé en ce qu'il comporte un dispositif de décodage conforme à l'une des revendications 19 à 24.

41. Ordinateur, caractérisé en ce qu'il comporte des moyens adaptés à mettre en œuvre le procédé d'insertion conforme à l'une des revendications 1 à 6.

25 42. Ordinateur, caractérisé en ce qu'il comporte un dispositif d'insertion conforme à l'une des revendications 7 à 13.

43. Ordinateur, caractérisé en ce qu'il comporte des moyens adaptés à mettre en œuvre le procédé de décodage conforme à l'une des revendications 14 à 18.

30 44. Ordinateur, caractérisé en ce qu'il comporte un dispositif de décodage conforme à l'une des revendications 19 à 24.

45. Scanner, caractérisé en ce qu'il comporte des moyens adaptés à mettre en œuvre le procédé d'insertion conforme à l'une des revendications 1 à 6.

5 46. Scanner, caractérisé en ce qu'il comporte un dispositif d'insertion conforme à l'une des revendications 7 à 13.

47. Scanner, caractérisé en ce qu'il comporte des moyens adaptés à mettre en œuvre le procédé de décodage conforme à l'une des revendications 14 à 18.

10 48. Scanner, caractérisé en ce qu'il comporte un dispositif de décodage conforme à l'une des revendications 19 à 24.

49. Appareillage d'imagerie médicale, et notamment appareil de radiographie aux rayons X, caractérisé en ce qu'il comporte des moyens adaptés à mettre en œuvre le procédé d'insertion conforme à l'une des revendications 1 à 6.

15 50. Appareillage d'imagerie médicale, et notamment appareil de radiographie aux rayons X, caractérisé en ce qu'il comporte un dispositif d'insertion conforme à l'une des revendications 7 à 13.

20 51. Appareillage d'imagerie médicale, et notamment appareil de radiographie aux rayons X, caractérisé en ce qu'il comporte des moyens adaptés à mettre en œuvre le procédé de décodage conforme à l'une des revendications 14 à 18.

52. Appareillage d'imagerie médicale, et notamment appareil de radiographie aux rayons X, caractérisé en ce qu'il comporte un dispositif de décodage conforme à l'une des revendications 19 à 24.

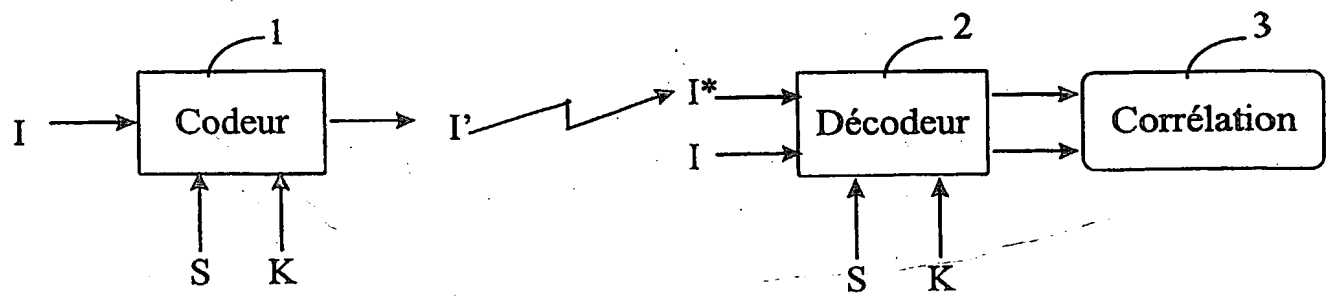


Figure 1

2/9

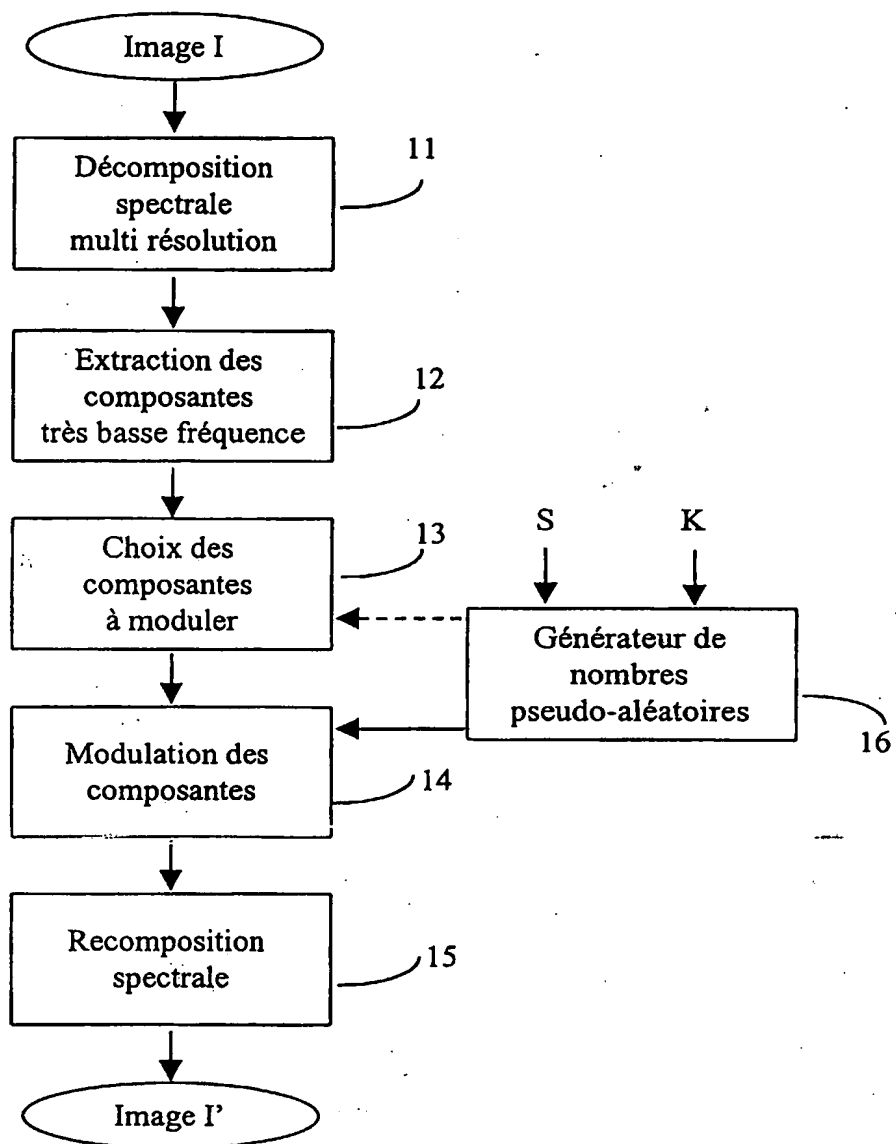


Figure 2

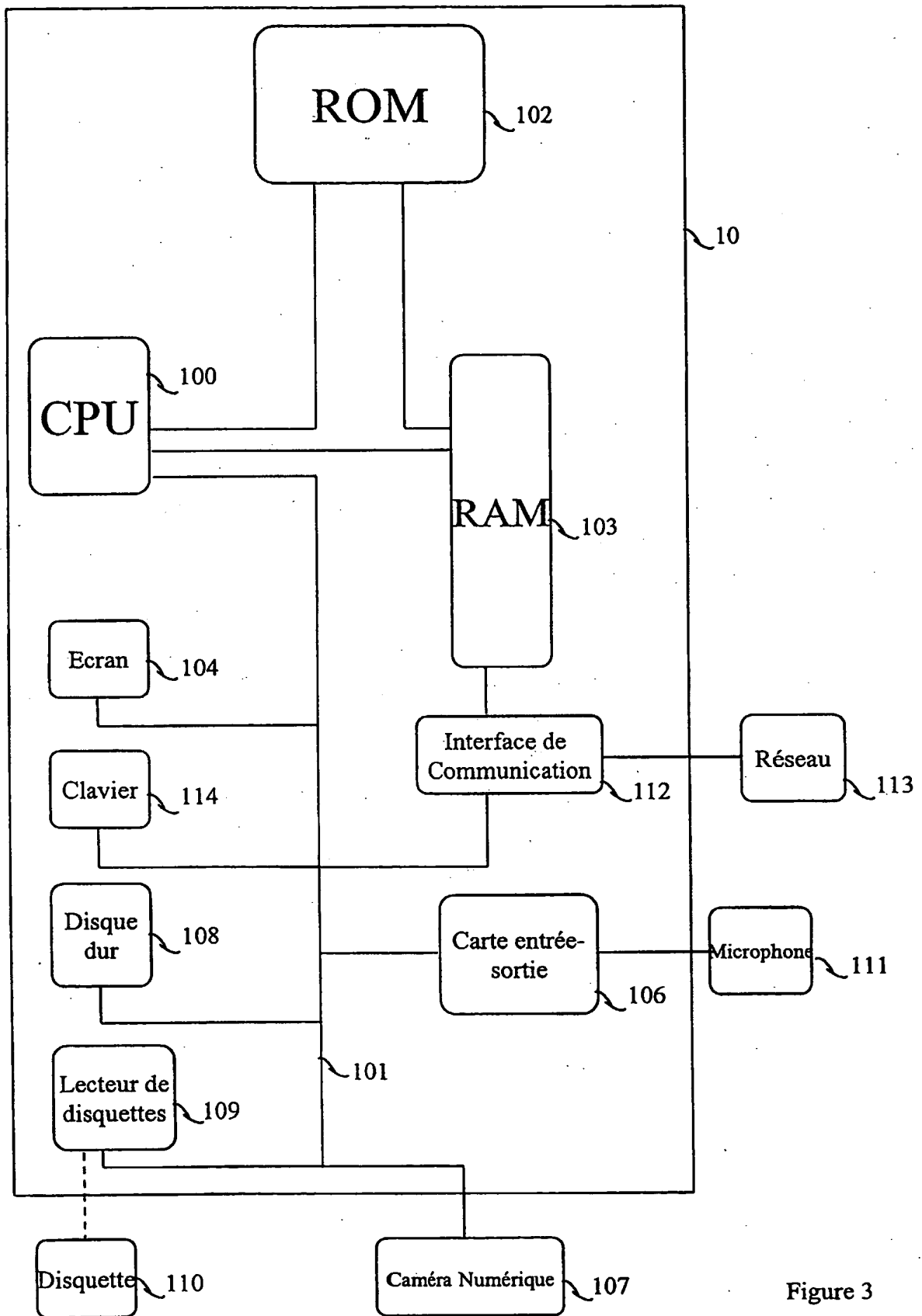


Figure 3

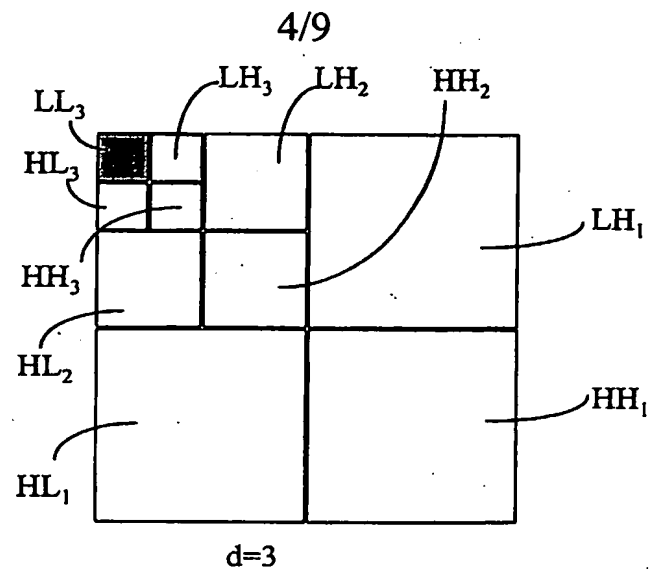


Figure 4

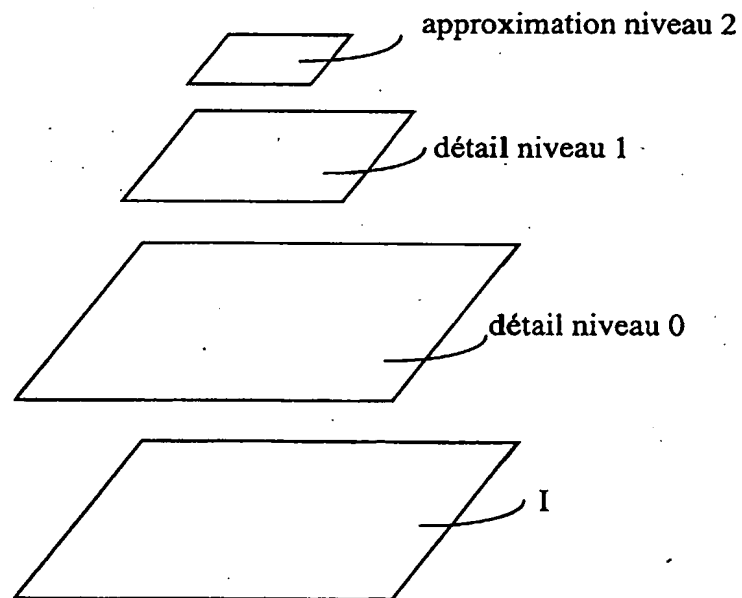
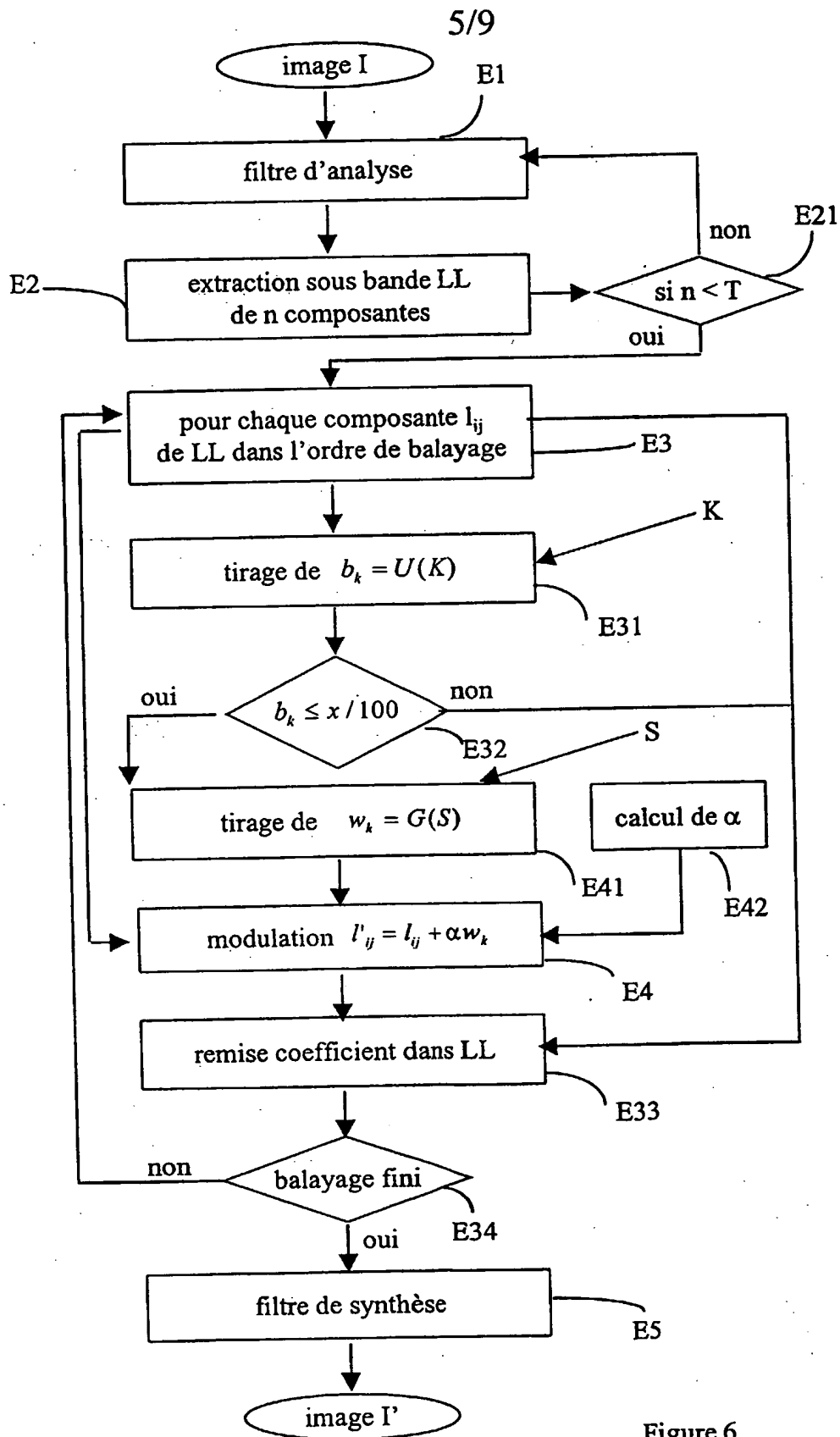


Figure 5



6/9

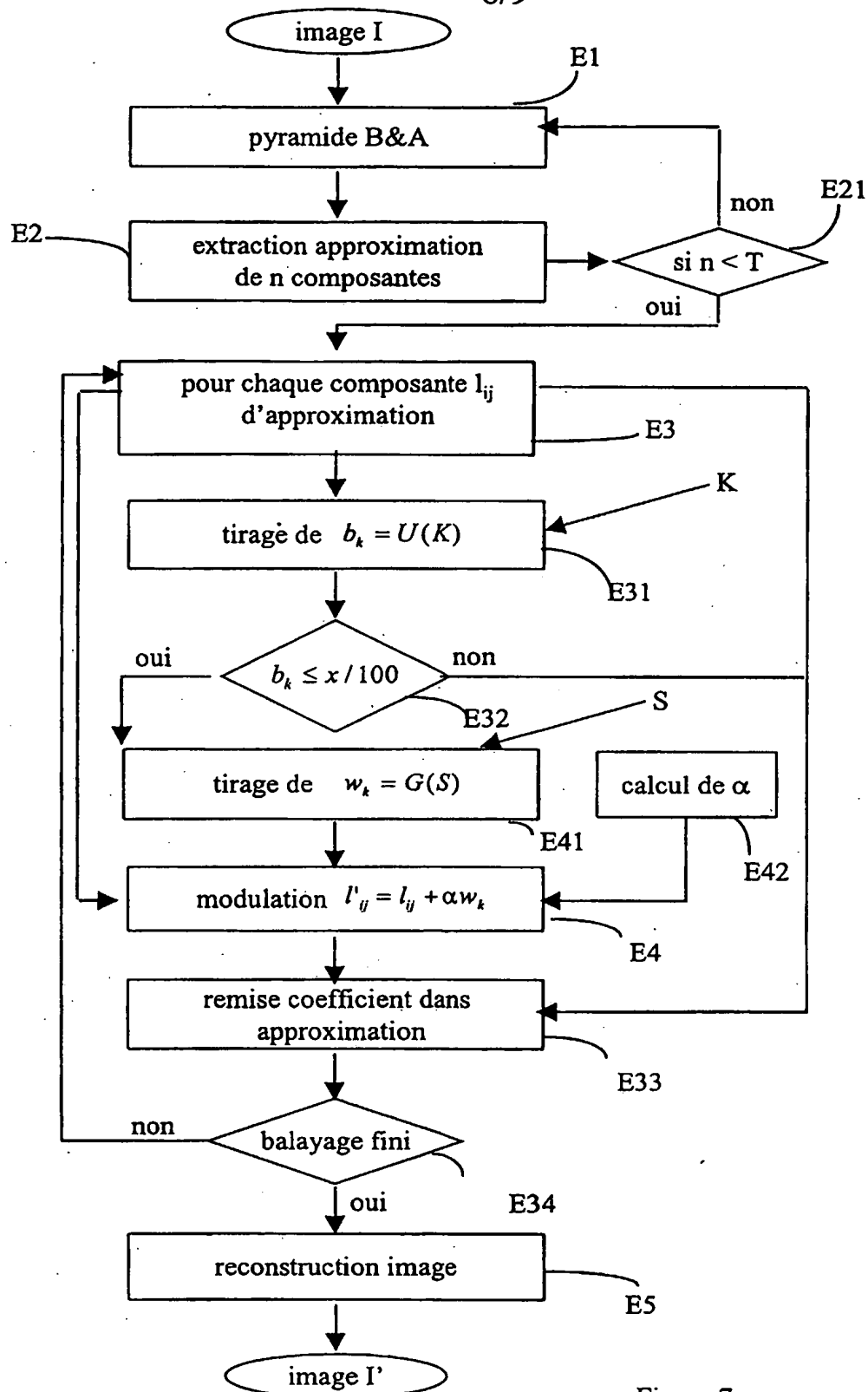


Figure 7

7/9

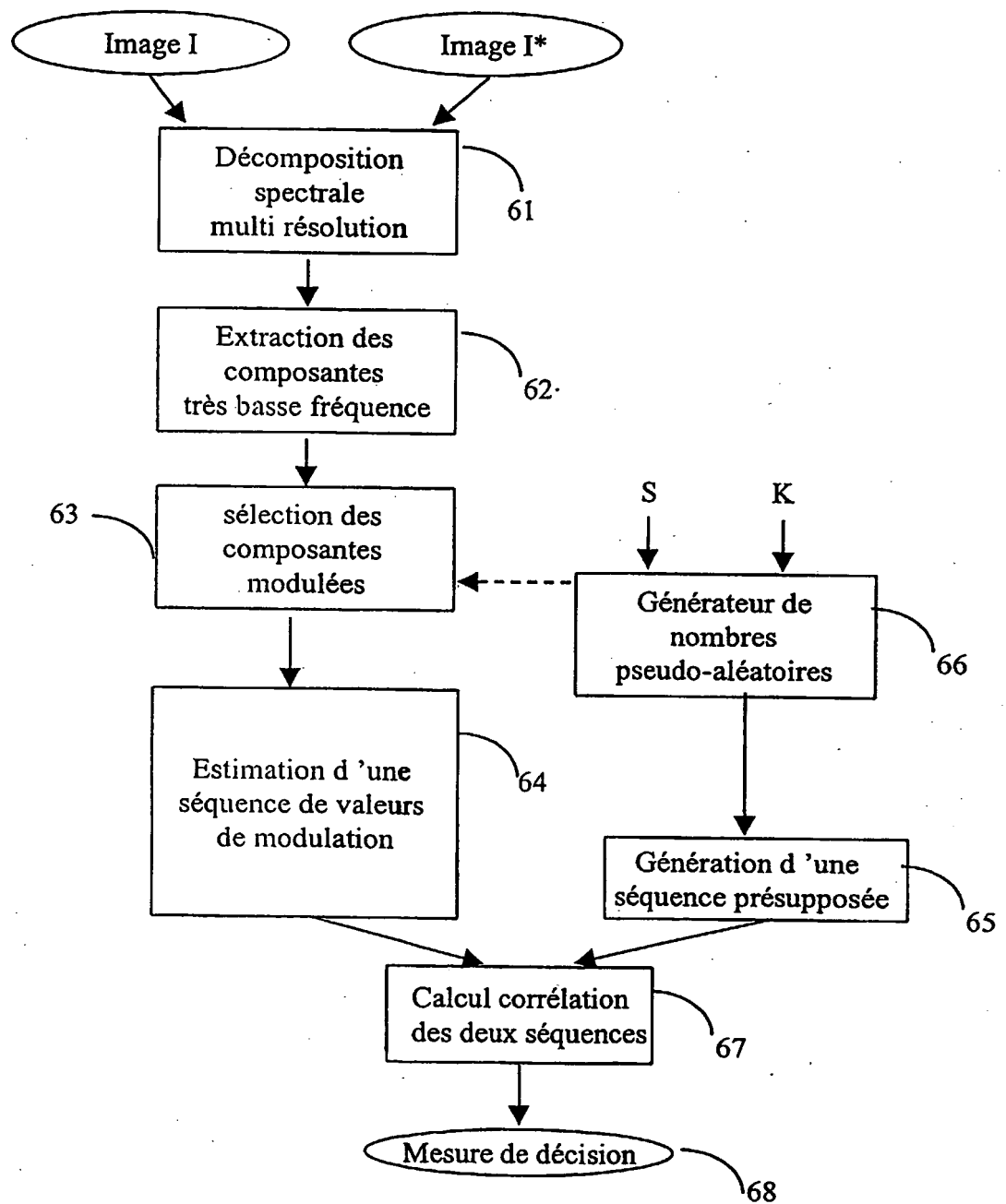


Figure 8

8/9

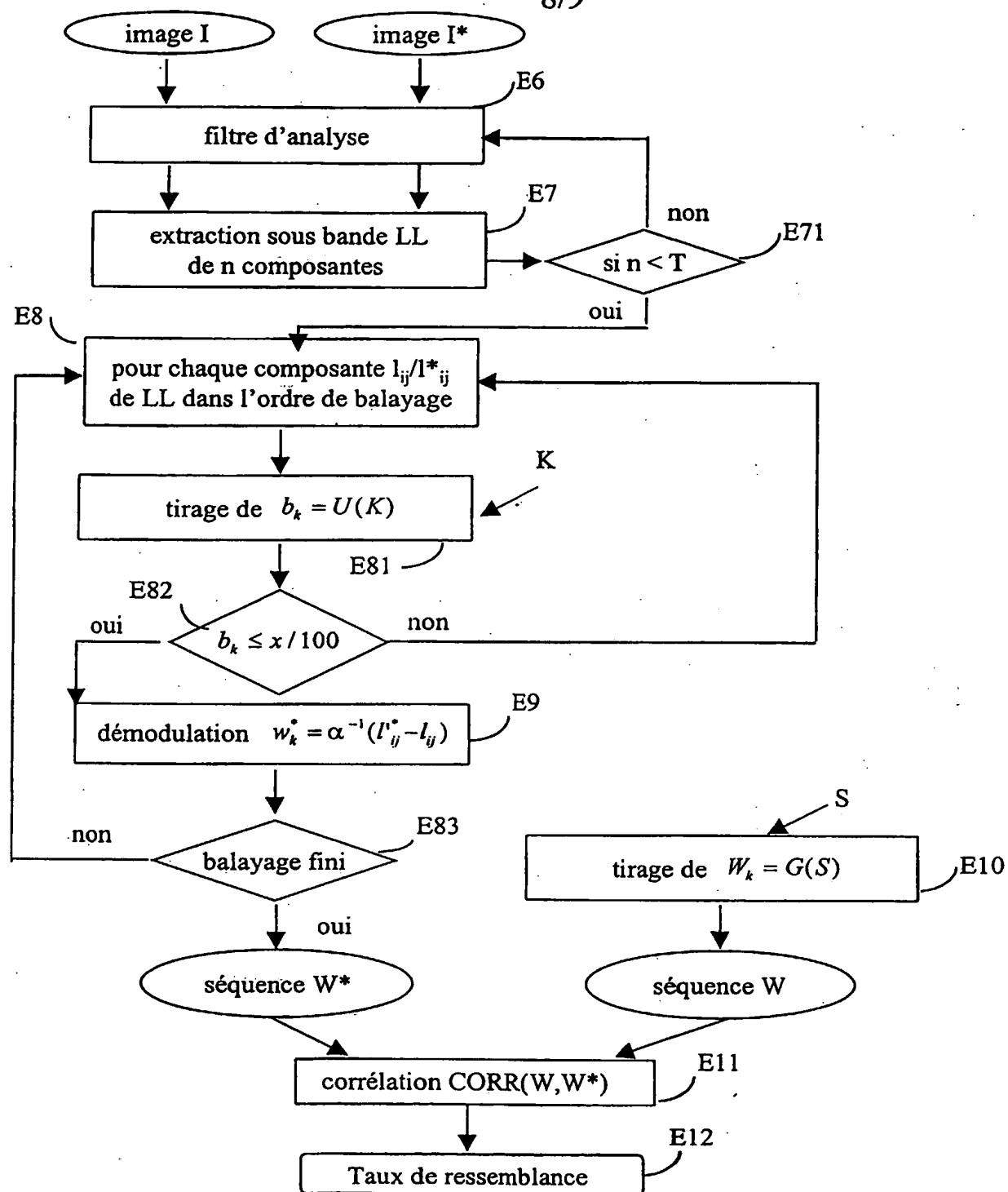


Figure 9

9/9

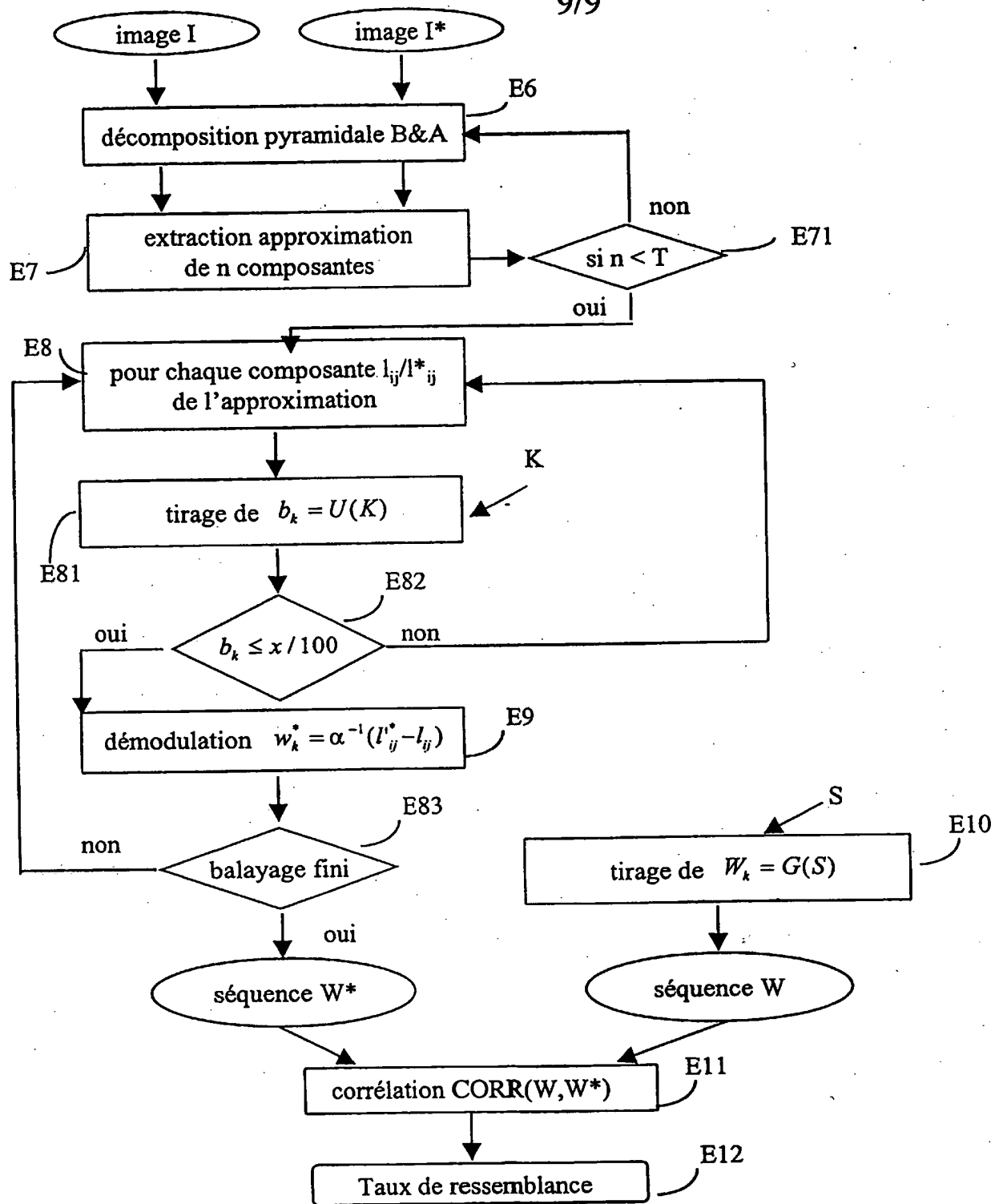


Figure 10

INSTITUT NATIONAL
de la
PROPRIETE INDUSTRIELLE

**RAPPORT DE RECHERCHE
PRELIMINAIRE**
établi sur la base des dernières revendications
déposées avant le commencement de la recherche

N° d'enregistrement
national

FA 565601
FR 9810149

DOCUMENTS CONSIDERES COMME PERTINENTS			Revendications concernées de la demande examinée
Catégorie	Citation du document avec Indication, en cas de besoin, des parties pertinentes		
Y	EP 0 840 513 A (NIPPON ELECTRIC CO) 6 mai 1998		1-3,5, 7-9,11, 14,15, 17,19, 20,22
A	* le document en entier *		4,6,10, 12,13, 16,18, 21,23-52
Y	EP 0 766 468 A (NIPPON ELECTRIC CO) 2 avril 1997		1-3,5, 7-9,11, 14,15, 17,19, 20,22
A	* le document en entier *		4,6,10, 12,13, 16,18, 21,23-52
A	US 5 530 759 A (MAGERLEIN KAREN A ET AL) 25 juin 1996 * colonne 1, ligne 11 - ligne 19 * * colonne 4, ligne 8 - ligne 26 *	25,33, 41,45	
A	EP 0 855 829 A (NOKIA TECHNOLOGY GMBH) 29 juillet 1998 * colonne 1, ligne 3 - ligne 35 *	25,29, 33,41	
A	RUANAIDH J J K O ET AL: "WATERMARKING DIGITAL IMAGES FOR COPYRIGHT PROTECTION" IEE PROCEEDINGS: VISION, IMAGE AND SIGNAL PROCESSING, vol. 143, no. 4, août 1996, pages 250-256, XP000627047 * le document en entier *		

DOMAINES TECHNIQUES
RECHERCHES (Int.CL.6)

H04N

2

EPO FORM 1503 03.82 (P04C13)

Date d'achèvement de la recherche

8 avril 1999

Examineur

Hubeau, R

CATEGORIE DES DOCUMENTS CITES

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un
autre document de la même catégorie
A : pertinent à l'encontre d'au moins une revendication
ou arrière-plan technologique général
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet bénéficiant d'une date antérieure
à la date de dépôt et qui n'a été publié qu'à cette date
de dépôt ou qu'à une date postérieure.
D : cité dans la demande
L : cité pour d'autres raisons
& : membre de la même famille, document correspondant

THIS PAGE BLANK (USPTO)